CLAIMS

1. A method of controlling the processing of data, wherein the data comprises a plurality of usage rules for a plurality of data items, and comprising applying individualised usage rules to each of the data items based on a measurement of integrity of a computing entity to which the data items are to be made available, such that the instantiation of the data at the computing entity depends on the integrity of the computing entity.

2. A method as claimed in claim 1, in which at least some of the usage rules comprise masking instructions for masking the associated data items.

3. A method as claimed in claim 2, in which a data item is masked from a set of data by encrypting it.

4. A method as claimed in claim 3, in which a data item is encrypted with an associated encryption key, said encryption key being different for different ones of the data items.

5. A method as claimed in claim 1, in which the usage rules define security rules for the associated data item.

6. A method as claimed in claim 1, in which the data may be transferred between a plurality of computing entities and the instantiation of the data at each computing entity depends on the capabilities of that entity.

7. A method as claimed in claim 6, in which a computing entity is a computing platform.

8. A method as claimed in claim 6, in which the computing entity is a software process.

9. A method as claimed in claim 1, in which a computing entity can reliably and irrevocably deny future access to selected data items.

10. A method as claimed in claim 9, in which means for accessing the data is stored within a protected memory.

11. A method as claimed in claim 10, in which the protected memory is within a trusted computing module.

12. A method as claimed in claim 1, in which computing entities negotiate with one another concerning the use of the data before the data is made available.

13. A method as claimed claim 1, in which the data has constraints defining conditions for use of the data.

14. A method as claimed in claim 13, in which the constraints define at least one item selected from:

a. the purpose for which the data can be used

b. the geographical area in which the data may be manifested

c. the temporal domain in which the data may be manifested

d. the computing platforms that may manipulate the data.

15. A method as claimed in claim 1 in which the data further includes test data.

16. A method as claimed in claim 15, in which the structure of test data is comparable to the structure of real data contained by the data items.

17. A method as claimed in claim 16, in which the results of operations performed on the test data are examined in order to make a decision on whether to release the real data to a node that operated on the test data.

18. A method as claimed in claim 1, in which a node requesting access to the data supplies hostage material to the node issuing the data prior to the issuance of the data.

19. A method as claimed in claim 18, in which a third party hostage release authority is contacted to activate the hostage material.

20. A method as claimed in claim 1 in which a node finding itself in possession of data whose history or content do not meet predetermined requirements, formats the data and places it in a repository.

21. A method as claimed in claim 20, in which the data placed in the repository is in an encrypted form.

22. A method as claimed in claim 21, in which the data is encrypted using a public key included in the data.

23. A method as claimed in claim 21 or 22, in which the data in the repository is associated with an identification means to enable the owner of the data to identify it.

24. A method as claimed in claim 1, in which a node wishing to present the data for retrieval places the data in a repository.

25. A method as claimed in claim 24, in which the data is placed in the repository in encrypted form.

26. A method as claimed in claim 25, in which the data is encrypted using a public key included in the data.

27. A method as claimed in claim 26, in which the data in the repository is associated with identification means to enable the owner of the data to identify it.

28. A method as claimed in claim 1, in which constraints associated with the data determine whether the data will process on anything other than a trusted computing platform.

29. A method as claimed in claim 28, in which constraints associated with the data determine whether the data and/or results from processing the data are inhibited from viewing by a computing platform owner or administrator.

30. A method as claimed in claim 1 in which the security contracts are stored separately from the data.

31. A method as claimed in claim 1 in which mask or decryption keys are stored separately from the data.

32. A method as claimed in claim 1 in which a computing entity that receives data signs the data with a signature key belonging to that entity.

33. A method of controlling the processing of data, wherein the data comprises a plurality of rules associated with a plurality of data items, said rules acting to define the use of the data or security to be observed when processing the data, and in which forwarding of the data is performed in accordance with mask means provided in association with the rules.

34. A method as claimed in claim 33, in which the mask comprises at least one of a symmetric encryption string, symmetric encryption key, and an asymmetric encryption key.

35. A method as claimed in claim 33, in which the rules associated with the data items are adhered to in preference to data handling rules associated with a computing entity processing the data.

36. A method as claimed in claim 33, in which at least some of the rules comprise masking instructions for masking the associated data items.

37. A method as claimed in claim 36, in which a data item is masked from a set of data by encrypting it.

38. A method as claimed in claim 37, in which a data item is encrypted with an associated encryption key, said encryption key being different for different ones of the data items.

39. A method as claimed in claim 33 in which the data may be transferred between computing entities and the instantiation of the data at each computing entity depends on the capabilities of the entity.

40. A method as claimed in claim 33, in which the rules define at least one item selected from:

a. the purpose for which the data can be used

b. the geographical area in which the data may be manifested

c. the temporal demain in which the data may be manifested

d. the computing platforms that may manipulate the data.

41. A method as claimed in claim 33 in which the data further includes test data, the test data is comparable to the structure of real data contained by the data items, and in which the results of operations performed on the test data are examined in order to make a decision on whether to release the real data to node that operated on t he test data.

42. A method as claimed in claim 33, in which a computing entity finding itself in possession of data whose history or content do not meet predetermined requirements, or wishing to make data available because it has performed some processing in at least partially masked form, formats the data places it in a repository.

43. A computer program for instructing a programmable computer to implement a method of controlling the processing of data, wherein the data comprises a plurality of usage rules for a plurality of data items, the programmable computer being programmed to apply individualised usage rules to each of the data items based on a measurement of integrity of a computing entity to which the data items are to be made available, such that the instantiation of the data at the computing entity depends on the integrity of the computing entity.

44. A processing system for processing private data, wherein the private data comprises a plurality of data fields and each field is associated with customisation data that controls the use and propagation of the data, and wherein the processing system is subservient to the constraints deferred by the customisation data.

45. A computing device arranged to receive data and security rules associated with the data, and in which forwarding of the data is performed in accordance with the

security rules, including encryption keys, supplied with the security rules instead of with keys belonging to the security device.

46. A method of controlling the processing of data, wherein the data comprises a plurality of usage rules for a plurality of data items, and the method comprising applying individualised usage rules to each of the data items based on a measurement of integrity of a computing entity to which the data items are to be made available in which at least some of the useage rules comprise masking instructions for masking the associated data items.

47. A method as claimed in claim 46, in which a data item is masked from a set of data by encrypting it.

48. A method as claimed in claim 47, in which a data item is encrypted with an associated encryption key, said encryption key being different for different ones of the data items.

49. A computer program for instructing a programmable computer to implement a method of controlling the processing of data, wherein the data comprises a plurality of rules associated with a plurality of data items, said rules acting to define the use of the data or security to be observed when processing the data, wherein the programmable computer is programmed to forward data in accordance with mask means provided in association with the rules.